

MINIMAL RAMIFICATION IN NILPOTENT EXTENSIONS

NADYA MARKIN AND STEPHEN V. ULLOM

ABSTRACT. Let G be a finite nilpotent group and K a number field with torsion relatively prime to the order of G . By a sequence of central group extensions with cyclic kernel we obtain an upper bound for the minimum number of prime ideals of K ramified in a Galois extension of K with Galois group isomorphic to G . This sharpens and extends results of Geyer and Jarden and of Plans. Also we confirm Boston's conjecture on the minimum number of ramified primes for a family of central extensions by the Schur multiplier.

1. INTRODUCTION

Given a number field K and a finite group G an important problem is to find a Galois extension L of K such that its Galois group $\text{Gal}(L/K)$ is isomorphic to G . Scholz and Reichardt (see Serre [12] for a modern account) proved independently that any l -group G , l an odd prime, occurs as the Galois group of an extension of the rationals. Shafarevic [13] has shown for any solvable group G and number field K that there exists a Galois extension L/K with $G \cong \text{Gal}(L/K)$. In this paper we ask for given K and nilpotent G , what is the minimum number $\text{minram}_K(G)$ of prime ideals of K ramified in L as L runs over extensions of K with $\text{Gal}(L/K) \cong G$? We rephrase the question for l -groups G : For a given finite set S of prime ideals of K , $K(l, S)$ denotes the maximal l -extension of K which is unramified outside S . How large must S be so that G is isomorphic to a quotient group of $\text{Gal}(K(l, S)/K)$ for some S ?

One knows $\text{minram}_{\mathbb{Q}}(G) \leq n$ if G is an l -group of order l^n , $l \neq 2$, cf. [12]. If G is an abelian group, an application of class field theory (Theorem 5.2) shows $\text{minram}_K(G) \leq d(G) :=$ minimum number of generators of G . In fact for the case when $K = \mathbb{Q}$, Boston's conjecture [1] stated below implies that $\text{minram}_{\mathbb{Q}}(G) \leq d(G)$ for all finite groups G .

Suppose G is a nilpotent group and the field K satisfies for each prime l dividing the order $|G|$ of G conditions

- (1) K does not contain a primitive l -th root of unity ζ_l
- (2) K has no ideal classes of order l^2 ,

then Theorem 8.4 states

$$\text{minram}_K(G) \leq \sum_{i \geq 1} d(G_i/G_{i+1}) + t(K).$$

Here $\{G_i\}$ is the lower central series of G , $G_1 = G$, $G_{i+1} = [G_i, G]$ and $t(K)$ is a constant depending only on K . This extends Plans' [10] result on $\text{minram}_{\mathbb{Q}}(G)$ to all number fields K satisfying (1), (2) above. Secondly, Geyer and Jarden [3] obtain

⁰AMS classification: 12F12, 11S31, 12F10, 11R32

Research supported by the Claude Shannon Institute, Science Foundation Ireland Grant 06/MI/006.

the bound $\minram_K(G) \leq n + t(K)$, where the l -group G has order l^n and $\zeta_l \notin K$. We obtain the improved bound by considering central embedding problems with a cyclic kernel, not just kernel of prime order as in [3]. Note that without condition (2), the methods of Section 8 still generalize the results of Geyer and Jarden [3] to nilpotent groups, giving a weaker bound for a nilpotent group G of order $\prod_{l||G|} l^{n_l}$, namely

$$\minram_K(G) \leq \max_{l||G|} \{n_l\} + t(K).$$

We generalize Geyer and Jarden's definition of an exceptional set T of primes to the prime power setting in Section 4; this provides the technical tool for constructing idele class characters with strictly controlled ramification.

The realization of l -groups is carried out in three steps similarly to [3], [12], [10]: the first step involves solving an embedding problem given a Scholz extension, in the second step we remove ramification in the solution outside the set of exceptional primes, and in the third step we force the solution to be Scholz at the cost of one extra ramifying prime. Finally in Section 8, for G nilpotent this prime is chosen to be the same for all primes l dividing the order of G .

We take another approach to the problem of realization of Galois groups with minimal ramification in Section 9. Take $K = \mathbb{Q}$ or an imaginary quadratic field with $\zeta_l \notin K$. We consider a family of l -extensions of K obtained from central extensions by the Schur multiplier and observe that a result of Fröhlich [2] for $K = \mathbb{Q}$ (extended to imaginary quadratic by Watt [14]) on realizing the Schur multiplier confirms Boston's conjecture 1.2 of [1] for groups corresponding to this family. This conjecture states that for any nontrivial finite group G , there exists an extension of \mathbb{Q} with Galois group G and exactly $\max(1, d(G^{ab}))$ ramified primes, and moreover no extension of \mathbb{Q} with Galois group G can be ramified at fewer than $\max(1, d(G^{ab}))$ primes (counting the infinite prime). See Kisilevsky-Sonn [6] for results on minimally ramified realization of semiabelian groups.

2. EMBEDDING PROBLEM

Fix an algebraic closure \bar{K} of a number field K and let $G_K = \text{Gal}(\bar{K}/K)$ denote the absolute Galois group of K . An *embedding problem* (G_K, ρ, α) for G_K (see e.g. [9]) is a diagram with an exact sequence of finite groups and epimorphism ρ .

$$(2.0.1) \quad \begin{array}{ccccccc} & & & & G_K & & \\ & & & \swarrow \phi & \downarrow \rho & & \\ 1 & \longrightarrow & C & \longrightarrow & G & \xrightarrow{\alpha} & \bar{G} \longrightarrow 1. \end{array}$$

A solution ϕ of the embedding problem is a homomorphism $\phi : G_K \rightarrow G$ such that $\alpha \circ \phi = \rho$; a solution is *proper* if ϕ is surjective. If G, \bar{G} are l -groups with the same number of generators, it is easily seen that every solution is proper. When the kernel group C is contained in the center of G , the embedding problem (2.0.1) is called a *central embedding problem*. Every nilpotent group can be realized as a Galois group by solving a sequence of central embedding problems. For every prime \mathfrak{p} of K , fix a prime of \bar{K} above \mathfrak{p} and let $D_{\mathfrak{p}}$ (resp. $I_{\mathfrak{p}}$) denote its decomposition (resp. inertia) subgroup in G_K .

Let

(2.0.2)

$$\begin{array}{ccccccc}
 & & & & D_{\mathfrak{p}} & & \\
 & & & \swarrow \phi_{\mathfrak{p}} & \downarrow \rho_{\mathfrak{p}} & \searrow & \\
 1 & \longrightarrow & C & \longrightarrow & G_{\mathfrak{p}} & \xrightarrow{\alpha_{\mathfrak{p}}} & \bar{G}_{\mathfrak{p}} \longrightarrow 1.
 \end{array}$$

denote the corresponding local embedding problem, where $\bar{G}_{\mathfrak{p}} = \rho(D_{\mathfrak{p}})$, $G_{\mathfrak{p}} = \alpha^{-1}(\bar{G}_{\mathfrak{p}})$, and $\alpha_{\mathfrak{p}}, \rho_{\mathfrak{p}}$ are restrictions of α, ρ .

In this paragraph we assume in 2.0.1 that G is an l -group and the kernel C has prime order; let S_0 be a finite set of primes of K containing the infinite primes, prime divisors of l , and prime divisors of a set of ideals representing the ideal classes of K . More generally when G is a nilpotent group in Section 8, the set S_0 contains in addition the divisors of the order of G . It is known, cf. [3], that a solution to a global embedding problem 2.0.1 exists if and only for every prime \mathfrak{p} of K there exists a solution to the local embedding problem 2.0.2. The local embedding problem is solvable if $\rho(I_{\mathfrak{p}}) = 1$, since $D_{\mathfrak{p}}/I_{\mathfrak{p}} \cong \hat{\mathbb{Z}}$ is a free group; the Scholz condition ensures solvability at the ramified primes. Let $Ram(\rho) = \{\mathfrak{p} \text{ of } K \mid \rho(I_{\mathfrak{p}}) \neq 1\}$.

Definition 2.1 (l^N -Scholz homomorphism, cf. 3.2 of [3]). Given a number field K , an l -group G and a positive integer N such that l^N is divisible by the exponent of G . Denote by T a set of l^N -exceptional primes as defined in Section 4.

An epimorphism $\phi : G_K \rightarrow G$ is l^N -Scholz if

- For $\mathfrak{p} \in Ram(\phi) \cup T$, $\phi(D_{\mathfrak{p}}) = \phi(I_{\mathfrak{p}})$.
- For $\mathfrak{p} \in Ram(\phi)$, the absolute norm $N(\mathfrak{p}) \equiv 1 \pmod{l^N}$.
- For $\mathfrak{p} \in S_0$, $\phi(D_{\mathfrak{p}}) = 1$.

The last condition is an example of local data of [3]. We will also say the extension L/K is l^N -Scholz, where L is the subfield of \bar{K} fixed by $\ker(\phi)$.

The definition of l^N -Scholz does not depend on the choice of prime of \bar{K} above each \mathfrak{p} . Clearly if a homomorphism ϕ is l^N -Scholz, then it is l^k -Scholz for all integers $k \leq N$.

3. EXISTENCE OF SOLUTIONS

Theorem 3.1 (Existence Theorem). *Let (G_K, ρ, α) be a central embedding problem, $\bar{G} = \rho(G_K)$ is an l -group, $C = \ker(\alpha)$ cyclic of order l^e . Suppose ρ is l^N -Scholz (exponent of G divides l^N) and $\zeta_l \notin K$. Then the embedding problem*

(3.0.3)

$$\begin{array}{ccccccc}
 & & & & G_K & & \\
 & & & \swarrow \psi_0 & \downarrow \rho & \searrow & \\
 1 & \longrightarrow & C & \longrightarrow & G & \xrightarrow{\alpha} & \bar{G} \longrightarrow 1.
 \end{array}$$

has a solution.

Proof:

If G is a split extension of \bar{G} , we may apply Proposition 5.3, so assume the extension is Frattini, i.e., C is contained in the Frattini subgroup of G . We may break 3.0.3 into a sequence of e embedding problems each with kernel group of order l , which

we may solve by Proposition 7.3 of [3] at the cost of one ramified prime at each step. We obtain an l^N -Scholz solution ψ_0 to 3.0.3 such that

$$\text{Ram}(\psi_0) \cup T = \text{Ram}(\rho) \cup T \cup \{e \text{ primes of } K\}$$

■

In sections 5-7 we will show that the embedding problem 3.0.3 has an l^N -Scholz solution at the cost of only one additional ramified prime (assuming K has no ideal classes of order l^2 if $|C| > l$).

4. EXCEPTIONAL SET OF PRIMES

The key Lemma 4.2 was originally proved by the first author in a different way in her thesis [8]. The lemma below generalizes results of Gras in [4] Ch. II, Theorem 6.3.2 and Lemma 4.1, p. 361 in [11].

Lemma 4.1. *Let L/K be a Galois l -extension, $\tilde{K} = K(\mu_m)$, $\tilde{L} = L(\mu_m)$, where m is a power of l . If $\zeta_l \notin K$, then the canonical map*

$$K^\times / K^{\times m} \rightarrow \tilde{L}^\times / \tilde{L}^{\times m}$$

is injective.

Proof:

From Kummer theory, we have $H^1(\text{Gal}(\tilde{K}/K), \mu_m) \cong K^\times / K^{\times m}$ and $H^1(\text{Gal}(\tilde{K}/\tilde{L}), \mu_m) \cong \tilde{L}^\times / \tilde{L}^{\times m}$, where \tilde{K} denotes an algebraic closure of K . The extensions $K \subseteq \tilde{L} \subseteq \tilde{K}$ give the following exact sequence of cohomology groups via the restriction-inflation maps

$$1 \rightarrow H^1(\text{Gal}(\tilde{L}/K), \mu_m^\gamma) \rightarrow H^1(\text{Gal}(\tilde{K}/K), \mu_m) \rightarrow H^1(\text{Gal}(\tilde{K}/\tilde{L}), \mu_m),$$

where $\gamma = \text{Gal}(\tilde{K}/\tilde{L})$. It suffices to prove $H^1(\text{Gal}(\tilde{L}/K), \mu_m^\gamma) = 0$; note $\mu_m^\gamma = \mu_m$. By a second application of the restriction-inflation sequence, now to the extensions $K \subseteq L \subseteq \tilde{L}$, we have the exact sequence

$$1 \rightarrow H^1(\Gamma/\Delta, \mu_m^\Delta) \rightarrow H^1(\Gamma, \mu_m) \rightarrow H^1(\Delta, \mu_m),$$

where $\Gamma = \text{Gal}(\tilde{L}/K)$, $\Delta = \text{Gal}(\tilde{L}/L)$. The cohomology group $H^1(\Gamma/\Delta, \mu_m^\Delta) = 0$ since $\mu_m^\Delta = \mu_m \cap L = \{1\}$ ($\zeta_l \notin K$ and L/K is an l -extension). Since Δ is cyclic, by Herbrand theory, the orders of the Tate cohomology groups $H^i(\Delta, \mu_m)$ are equal for $i = 0, 1$. But $H^0(\Delta, \mu_m) = \mu_m^\Delta / \text{Norms} = 0$. This completes the proof. ■

Let K_S be the group of S -units of K , where S contains the infinite primes of K . By Dirichlet's unit theorem, the \mathbb{Z} -rank of K_S is

$$u := \text{rk}_{\mathbb{Z}}(K_S) = |S| - 1.$$

Lemma 4.2. *Assume $\zeta_l \notin K$. With the notation of Lemma 4.1 let M be an abelian extension of L containing \tilde{L} . There are isomorphisms*

$$\text{Gal}(\tilde{K}(\sqrt[m]{K_S})/\tilde{K}) \xrightarrow{f_1} \text{Gal}(\tilde{L}(\sqrt[m]{K_S})/\tilde{L}) \xrightarrow{f_2} \text{Gal}(M(\sqrt[m]{K_S})/M) \cong (\mathbb{Z}/m\mathbb{Z})^u.$$

Proof:

Apply Lemma 4.1 restricted to the image of K_S in \tilde{L}^\times to conclude that f_1 is an isomorphism. Next we show f_2 is an isomorphism. Let $F = \tilde{L}(\sqrt[l]{K_S}) \cap M$. We show $F = \tilde{L}$, so that f_2 would be an isomorphism. Since $F \subset M$, the extension F/L is abelian. And $\tilde{L} \subset F \subset L(\sqrt[l]{K_S})$. If F is not \tilde{L} , then F contains a cyclic extension F_0/\tilde{L} , $[F_0 : \tilde{L}] = l$. From Kummer theory, $F_0 = \tilde{L}(\sqrt[l]{b})$, $b \in K_S$. But $\text{Gal}(\tilde{L}(\sqrt[l]{b})/\tilde{L})$ is not abelian, thus $F = \tilde{L}$. ■

The corollary below will be used in section 8. We include it here for convenience.

Corollary 4.3. *Let K be a number field, S a finite set of primes of K and let $a > 1$ be an integer. For each $l \mid a$ let L_l/K be a Galois l -extension. Suppose that $\zeta_l \notin K$ for each $l \mid a$. Set $M_l = L_l(\zeta_{l^N}, \zeta_a)$ and $M = \prod_l M_l$. Then we have a series of isomorphisms:*

$$\begin{aligned} \text{Gal}(K(\sqrt[l^N]{K_S})/K(\zeta_{l^N})) &\cong \text{Gal}(L_l(\sqrt[l^N]{K_S})/L_l(\zeta_{l^N})) \\ &\cong \text{Gal}(M_l(\sqrt[l^N]{K_S})/M_l) \cong \text{Gal}(M(\sqrt[l^N]{K_S})/M) \end{aligned}$$

The diagram below contains the fields involved in these isomorphisms.

$$\begin{array}{ccccccc} K(\sqrt[l^N]{K_S}) & \longrightarrow & L_l(\sqrt[l^N]{K_S}) & \longrightarrow & M_l(\sqrt[l^N]{K_S}) & \longrightarrow & M(\sqrt[l^N]{K_S}) \\ \uparrow & & \uparrow & & \uparrow & & \uparrow \\ K(\zeta_{l^N}) & \longrightarrow & L_l(\zeta_{l^N}) & \longrightarrow & M_l & \longrightarrow & M \end{array}$$

Proof:

The first two isomorphisms follow from Lemma 4.2. To show the rightmost isomorphism note that $M_l(\sqrt[l^N]{K_S})/M_l$ is an l -extension, while $l \nmid [M : M_l]$. ■

Lemma 4.4. *For each $l \mid a$, assume that $\zeta_l \notin K$. Let R_l denote the field $L_l(\sqrt[l^N]{K_S})$ and let $\sigma_l \in \text{Gal}(R_l/L_l(\mu_{l^N}))$. Define $R = \prod_{l \mid a} R_l$. Then there exists $\sigma \in \text{Gal}(R/K(\mu_a))$ such that $\sigma|_{R_l} = \sigma_l$ for all $l \mid a$.*

Proof:

By Lemma 4.3, each σ_l extends to an element, say $\hat{\sigma}_l$, of $\text{Gal}(R_l M_l/M_l)$. The latter group is a subgroup of the l -group $\text{Gal}(R_l M_l/K(\mu_a))$. Now observe that $\text{Gal}(R/K(\mu_a)) \cong \prod_{l \mid a} \text{Gal}(R_l M_l/K(\mu_a))$. Therefore we may define $\sigma \in \text{Gal}(R/K(\mu_a))$ as $\sigma = \prod_{l \mid a} \hat{\sigma}_l$. ■

For an abelian group A and a prime number l , let $A_l = \{a \in A \mid a^l = 1\}$. We define the subgroup $V(l)$ (denoted by V when the prime l is implicit) of K^\times

$$V = \{a \in K^\times \mid (a) = \mathfrak{a}^l \text{ for a fractional ideal } \mathfrak{a} \text{ of } K\}.$$

We have the following split exact sequence, e.g. pg. 109 of [7],

$$1 \rightarrow E/E^l \rightarrow V/K^{\times l} \rightarrow Cl(K)_l \rightarrow 1,$$

where E denotes the group of units of K and the right hand map sends $a \bmod K^{\times l}$ to the ideal class of \mathfrak{a} , where $(a) = \mathfrak{a}^l$. Similarly

$$1 \rightarrow E/E^{l^N} \rightarrow EV^{l^{N-1}}/K^{\times l^N} \rightarrow Cl(K)_l \rightarrow 1.$$

Let w_1, \dots, w_s be a \mathbb{Z} -basis of $E \bmod$ torsion. As in [3], choose ideles $\alpha_1, \dots, \alpha_r \in J$ whose images are an \mathbb{F}_l -basis of the l -torsion subgroup $(J/K^{\times}U)_l$ of the ideal class group of K . Then for $j = 1, \dots, r$

$$\alpha_j^l = a_j^{-1} \epsilon_j, \quad a_j \in K^{\times}, \epsilon_j = (\epsilon_{j,v}) \in U, \epsilon_{j,v} \in U_v.$$

For all j and all primes v of K , a_j and $\epsilon_{j,v}$ have the same image in U_v/U_v^l . Taken $\bmod K^{\times l}$, the set $\{w_1, \dots, w_s, a_1, \dots, a_r\}$ is a basis of $V/K^{\times l}$.

We define a governing field Ω_l (compare Chapter 5 of [4] or [3] for $N = 1$)

$$(4.0.4) \quad \Omega_l = K(\mu_{l^N}, \sqrt[l^N]{EV^{l^{N-1}}}) = K(\mu_{l^N}, \sqrt[l^N]{E}, \sqrt[l^N]{V}) = \\ K(\mu_{l^N}, \sqrt[l^N]{w_i}, \sqrt[l^N]{a_j} : 1 \leq i \leq s, 1 \leq j \leq r).$$

It follows from lemma 4.2 that the Kummer extension satisfies $Gal(\Omega_l/K(\mu_{l^N})) \cong (\mathbb{Z}/l^N\mathbb{Z})^s \oplus (\mathbb{Z}/l\mathbb{Z})^r$. Of course, if $K = \mathbb{Q}$, we have $r = s = 0$.

Define subfields of Ω_l

$$N_i = K(\mu_{l^N}, \sqrt[l^N]{w_k} : 1 \leq k \leq s, k \neq i; \sqrt[l^N]{a_k} : 1 \leq k \leq r), \quad 1 \leq i \leq s$$

$$N'_j = K(\mu_{l^N}, \sqrt[l^N]{E}; \sqrt[l^N]{a_k} : 1 \leq k \leq r, k \neq j), \quad 1 \leq j \leq r.$$

Then $Gal(\Omega_l/N_i)$ is cyclic of order l^N while $Gal(\Omega_l/N'_j)$ has order l .

Definition 4.5 (cf. (5.5) of [3] for $N = 1$). A set $T_l = \{\mathfrak{p}_1, \dots, \mathfrak{p}_s, \mathfrak{q}_1, \dots, \mathfrak{q}_r\}$ of prime ideals of K such that $T_l \cap S_0 = \emptyset$ is l^N -exceptional if

$$Gal(\Omega_l/N_i) = D_{\mathfrak{p}_i}(\Omega_l/K), \quad 1 \leq i \leq s \quad \text{and}$$

$$Gal(\Omega_l/N'_j) = D_{\mathfrak{q}_j}(\Omega_l/K), \quad 1 \leq j \leq r.$$

Note that this property is independent of the primes above \mathfrak{p}_i (resp. \mathfrak{q}_j) since N_i (resp. N'_j) is a normal extension of K .

For a prime ideal \mathfrak{p} of K unramified in a Galois extension F/K , $Frob(\mathfrak{p}, F/K)$ denotes the conjugacy class in $Gal(F/K)$ consisting of the Frobenius elements of all prime ideals of F above \mathfrak{p} .

Choose

$$\sigma_i(l) \in Frob(\mathfrak{p}_i(l), \Omega_l/K), \quad 1 \leq i \leq s \quad \text{and}$$

$$\tau_j(l) \in Frob(\mathfrak{q}_j(l), \Omega_l/K), \quad 1 \leq j \leq r_l;$$

here we make the dependence on l explicit. Note that $\{\sigma_i(l), \tau_j(l) : 1 \leq i \leq s, 1 \leq j \leq r_l\}$ are a minimal generating set of the abelian group $Gal(\Omega_l/K(\mu_{l^N}))$. Further if a is the product of the primes dividing $|G|$, the latter group is isomorphic to $Gal(\Omega_l(\mu_{a^N})/K(\mu_{a^N}))$ by Lemma 4.2.

By the Chebotarev density theorem, there exists an l^N -exceptional set of primes disjoint from any given set of primes of K of density 0. Note that since v splits completely in $K(\mu_{l^N})/K$ for all $v \in T_l$, we have $\zeta_{l^N} \in K_v$ for all $v \in T_l$.

It follows from Kummer theory for primes $\mathfrak{p}_i, \mathfrak{q}_j \in T_l$ that

- w_i not an l -th power in $U_{\mathfrak{p}_i}$

- $w_i \in U_v^{l^N} \quad \forall v \in T_l, \quad v \neq \mathfrak{p}_i.$
- a_j not an l -th power in $U_{\mathfrak{q}_j}$
- $a_j \in U_v^l \quad \forall v \in T_l, \quad v \neq \mathfrak{q}_j.$

Note that if T_l is l^N -exceptional, then T_l is l^k -exceptional for all $1 \leq k \leq N$. We will therefore fix a set T_l of l^N -exceptional primes, where l^N is divisible by the exponent of the l -group G . From now on until section 8 we will let T denote T_l , as the prime l is implicit.

5. SPLIT CASE

We begin with a lemma which generalizes Lemma 4.2 of [3]. If $K = \mathbb{Q}$, and b is an integer greater than one, the lemma follows at once from the fact there are infinitely many primes $q \equiv 1 \pmod{b}$, and we take subfield M of $\mathbb{Q}(\mu_q)$ of degree b .

Lemma 5.1. *Given integer $b > 1$ and number field K , there exist infinitely many prime ideals \mathfrak{q} of K and cyclic extensions $M = M(\mathfrak{q})$ of K of degree b such that \mathfrak{q} is the unique ramified prime of M/K , \mathfrak{q} is totally ramified, and \mathfrak{q} does not divide b .*

Proof:

Let S be a finite set of primes of K containing S_0 and prime divisors of b and let $\Omega = K(\sqrt[b]{K_S})$. By Chebotarev's theorem there exist infinitely many primes \mathfrak{q} of K , $\mathfrak{q} \notin S$, such that \mathfrak{q} splits completely in Ω/K . For such \mathfrak{q} , Ω is contained in the completion $K_{\mathfrak{q}}$ and so $K_S \subset (K_{\mathfrak{q}}^{\times})^b$.

Define $J_S = \prod_{v \in S} K_v^{\times} \times \prod_{v \notin S} U_v \subset J$. By class field theory, cyclic extensions of K are given by idele class characters. Since $J/K^{\times} \cong J_S/K_S$, we want to define an epimorphism $\chi : J_S/K_S \rightarrow \mu_b$ with $\chi(K_S) = \{1\}$. The group $U_{\mathfrak{q}}/U_{\mathfrak{q}}^b$ is cyclic of order b , so there is an epimorphism $\chi_{\mathfrak{q}} : U_{\mathfrak{q}} \rightarrow \mu_b$ with kernel $U_{\mathfrak{q}}^b$. For $\alpha = (\alpha_v) \in J_S$, define $\chi(\alpha) = \chi_{\mathfrak{q}}(\alpha_{\mathfrak{q}})$. Note $\chi(K_S) = \{1\}$ and $\chi(K_v^{\times}) = \{1\}$, $v \in S$. By class field theory, χ corresponds to a cyclic, degree b extension $M(\mathfrak{q})/K$ in which \mathfrak{q} is totally and tamely ramified and the other primes of K are unramified. ■

Theorem 5.2. *Let A be a finite abelian group with d generators. There exist infinitely many Galois extensions N/K such that $\text{Gal}(N/K) \cong A$ and exactly d primes of K ramify in N . Such N is its own genus field relative to K .*

Proof:

Write A as a direct product of d cyclic groups and apply Lemma 5.1 to each factor. The resulting extensions $M(\mathfrak{q}_i)$, $1 \leq i \leq d$ are linearly disjoint over K by ramification considerations. Take N to be the composite of the fields $M(\mathfrak{q}_i)$. Note that these \mathfrak{q}_i 's are not to be confused with the ones defined in Definition 4.5. ■

Proposition 5.3 (Split Case). *Let G be an l -group of exponent dividing l^N . Suppose the homomorphism $\rho : G_K \rightarrow \bar{G}$ is l^N -Scholz and the central exact sequence is split*

$$1 \rightarrow C \rightarrow G \rightarrow \bar{G} \rightarrow 1,$$

where the kernel C of $\alpha : G \rightarrow \bar{G}$ is cyclic. There is an l^N -Scholz solution ϕ to the embedding problem (G_K, ρ, α) and a prime \mathfrak{q} not in $S = \text{Ram}(\rho) \cup S_0 \cup T$ such that $\text{Ram}(\phi) = \text{Ram}(\rho) \cup \{\mathfrak{q}\}$.

Proof:

We apply the argument in Lemma 5.1 with $b = |C|$, $\Omega = L(\mu_{l^N}, \sqrt[b]{K_S})$, where L is the subfield of \bar{K} fixed by $\ker(\rho)$, to obtain \mathfrak{q} and an idele class character χ of order b ; \mathfrak{q} splits completely in Ω/K . By the Reciprocity law χ corresponds to an epimorphism $\eta : G_K \rightarrow C$. Then $\phi = (\rho, \eta) : G_K \rightarrow \bar{G} \times C$, $\sigma \mapsto (\rho(\sigma), \eta(\sigma))$, is a proper solution to the embedding problem. It remains to check that ϕ is l^N -Scholz, given that ρ is l^N -Scholz.

If $v \in S_0$, $\phi(D_v) = 1$ since $\rho(D_v) = 1$ (given) and $\eta(D_v) = 1$ for $v \in S$. If $v \in T$, $\phi(D_v) = \phi(I_v)$ since $\rho(D_v) = \rho(I_v)$ (given) and $\eta(D_v) = 1$ for $v \in S$.

Suppose $v \in \text{Ram}(\phi) = \text{Ram}(\rho) \cup \{\mathfrak{q}\}$.

If $v = \mathfrak{q}$, \mathfrak{q} splits completely in $K(\mu_{l^N})/K$, hence $N(\mathfrak{q}) \equiv 1 \pmod{l^N}$. Since \mathfrak{q} splits completely in L/K , $\rho(D_{\mathfrak{q}}) = 1$. As $\eta(I_{\mathfrak{q}}) = C$ for $\eta : G_K \rightarrow C$, we have $\eta(D_{\mathfrak{q}}) = \eta(I_{\mathfrak{q}})$. Thus $\phi(D_{\mathfrak{q}}) = \phi(I_{\mathfrak{q}})$.

If $v \in \text{Ram}(\rho)$, then $N(v) \equiv 1 \pmod{l^N}$ and $\rho(D_v) = \rho(I_v)$ (given). But $\eta(D_v) = 1$ since $v \in \text{Ram}(\rho) \subset S$. Thus $\phi(D_v) = \phi(I_v)$ for $v \in \text{Ram}(\phi)$.

We conclude $\phi = (\rho, \eta)$ is an l^N -Scholz solution with one additional ramified prime. \blacksquare

6. REMOVING RAMIFICATION

Lemma 6.1. *Let K be a number field not containing ζ_l , $N \geq e \geq 1$. Given a finite set S of primes disjoint from an l^N -exceptional set T , characters $\chi_v : U_v \rightarrow \mu_{l^e}$, for $v \in S$, at least one of which is onto. Assume K has no ideal classes of order l^2 when $e > 1$. There exists an idele class character $\chi : J/K^\times \rightarrow \mu_{l^e}$ such that $\chi|_{U_v} = \chi_v$ for all $v \in S$ and $\chi|_{U_v} = 1$ for all $v \notin S \cup T$.*

Proof:

It suffices to prove the result when $S = \{v_0\}$ and then take the product of the resulting characters. Let $I = T \cup \{v_0\}$.

Step 1: Defining f on UK^\times/K^\times .

We define an epimorphism $f : U \rightarrow \mu_{l^e}$ of the form

$$f = \prod_{v \in I} \chi_v,$$

with $f|_{U_v} = 1$ for $v \notin I$. The character χ_{v_0} is given and the characters χ_v , $v \in T$, are to be defined suitably. Each character χ_v is trivial for $v \notin I$.

By the definition of an l^N -exceptional set of primes, the image of each unit w_i generates $U_{\mathfrak{p}_i}/U_{\mathfrak{p}_i}^{l^e}$, $\mathfrak{p}_i \in T$, hence we can define $\chi_{\mathfrak{p}_i} : U_{\mathfrak{p}_i} \rightarrow \mu_{l^e}$, $1 \leq i \leq s$, to satisfy

$$\chi_{\mathfrak{p}_i}(w_i)\chi_{v_0}(w_i) = 1.$$

Similarly $\epsilon_{j, \mathfrak{q}_j}$ generates $U_{\mathfrak{q}_j}/U_{\mathfrak{q}_j}^l$ (hence also modulo $U_{\mathfrak{q}_j}^{l^e}$) and we can define $\chi_{\mathfrak{q}_j} : U_{\mathfrak{q}_j} \rightarrow \mu_{l^e}$, $1 \leq j \leq r$, to satisfy

$$\chi_{\mathfrak{q}_j}(\epsilon_{j, \mathfrak{q}_j})\chi_{v_0}(\epsilon_{j, v_0}) = 1.$$

Next we establish the "off-diagonal" vanishing of $\prod_{v \in I} \chi_v$. Recall that $\epsilon_{j,v} \in U_v^l$ for $\mathfrak{q}_j \neq v \in T$ for each j , and $w_i \in U_v^{l^e}$ for $\mathfrak{p}_i \neq v \in T$ for each i . Thus we have

$$\prod_{v \in I} \chi_v(w_i) = \chi_{\mathfrak{p}_i}(w_i) \chi_{v_0}(w_i) \prod_{\mathfrak{p}_i \neq v \in T} \chi_v(w_i) = 1,$$

$$\prod_{v \in I} \chi_v(\epsilon_{j,v}^{l^{e-1}}) = \chi_{\mathfrak{q}_j}(\epsilon_{j,\mathfrak{q}_j}^{l^{e-1}}) \chi_{v_0}(\epsilon_{j,v_0}^{l^{e-1}}) \prod_{\mathfrak{q}_j \neq v \in T} \chi_v(\epsilon_{j,v}^{l^{e-1}}) = 1.$$

It follows that $\prod_{v \in I} \chi_v$ is trivial on the image of $E \oplus (\oplus_{j=1}^r \langle \epsilon_j \rangle)$ in $\prod_{v \in I} U_v / U_v^{l^e}$. Letting $\Delta : K^\times \rightarrow J$ be the diagonal embedding, we have in particular $f(\Delta(E)) = 1$, so f is defined on $U/\Delta(E)$, which we write as $U/E \cong UK^\times/K^\times$.

Note if l does not divide the class number of K , then f already provides the desired idele class character since the l -part of the ideal class group $J/K^\times U$ will be trivial. Otherwise we must extend f from $K^\times U/K^\times$ to J/K^\times .

Step 2: Character of order l .

Define $f_1 : U \rightarrow \mu_l$ by $f_1 = f^{l^{e-1}}$. By the techniques of the proof of Lemma 6.1 of [3], f_1 extends to an idele class character χ_1 of order l with $\chi_1|_{U_v} = \chi_v^{l^{e-1}}$, for $v \in I$ and $\chi_1|_{U_v} = 1$ if $v \notin I$. This follows from the trivial fact that an l^e -exceptional set T is l -exceptional.

We have $\frac{K^\times U}{K^\times \ker(f_1)} \cap \frac{K^\times \ker(\chi_1)}{K^\times \ker(f_1)} \equiv 1$. Also we have $|J/K^\times \ker(f_1)| = |J/K^\times U| \cdot |K^\times U/K^\times \ker(f_1)| = h \cdot l$, where h is the class number of K , which we may assume is a power of l . Thus $|K^\times \ker(\chi_1)/K^\times \ker(f_1)| = \frac{|J/K^\times \ker(f_1)|}{|J/K^\times \ker(\chi_1)|} = \frac{h \cdot l}{l} = |J/K^\times U|$. This implies that the following exact sequence

$$1 \rightarrow \frac{K^\times U}{K^\times \ker(f_1)} \rightarrow \frac{J}{K^\times \ker(f_1)} \rightarrow J/K^\times U \rightarrow 1$$

splits, with $\frac{K^\times \ker(\chi_1)}{K^\times \ker(f_1)}$ mapping isomorphically onto $J/K^\times U$. The image $J/K^\times U$ has exponent l by assumption and the kernel is cyclic of order l . Hence $\frac{J}{K^\times \ker(f_1)}$ has exponent l .

Step 3: Extending to a character of order l^e .

First we prove the following claim about finite abelian l -groups.

Claim 6.2. Let Γ be a finite abelian l -group and let $\gamma \subseteq \Gamma$ be a cyclic subgroup of order l^e . If Γ/γ^l has exponent l , then γ is a direct summand of Γ .

Proof:

The exponent of Γ is l^e , since for any element $g \in \Gamma$ we have $g^l \in \gamma^l$ and hence $g^{l^e} = 1$. Therefore γ is a subgroup generated by an element of maximal order, and hence is a direct summand, as desired.

We have the following diagram with exact rows and columns

$$\begin{array}{ccccccc}
& & 1 & & 1 & & \\
& & \downarrow & & \downarrow & & \\
& & \frac{(K^\times U)^l K^\times \ker(f)}{K^\times \ker(f)} & \xrightarrow{=} & \frac{(K^\times U)^l K^\times \ker(f)}{K^\times \ker(f)} & & \\
& & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \frac{K^\times U}{K^\times \ker(f)} & \longrightarrow & J/K^\times \ker(f) & \longrightarrow & J/K^\times U \longrightarrow 1 \\
& & \downarrow & & \downarrow & & \downarrow \cong \\
1 & \longrightarrow & \frac{K^\times U}{K^\times \ker(f_1)} & \longrightarrow & J/K^\times \ker(f_1) & \longrightarrow & J/K^\times U \longrightarrow 1 \\
& & \downarrow & & \downarrow & & \\
& & 1 & & 1 & &
\end{array}$$

We apply Claim 6.2 with $\gamma = \frac{K^\times U}{K^\times \ker(f)}$ and $\Gamma = \frac{J}{K^\times \ker(f)}$. It follows from the diagram above that $\Gamma/\gamma^l \cong \frac{J}{K^\times \ker(f_1)}$, which by assumption has exponent l . Claim 6.2 implies that $\frac{K^\times U}{K^\times \ker(f)}$ is a direct summand of $\frac{J}{K^\times \ker(f)}$. Thus f extends to a character

$$\chi : J/K^\times \rightarrow \mu_{l^e}$$

by defining χ equal to f on U and χ trivial on a complement of $K^\times U/K^\times \ker(f)$. ■

Theorem 6.3 (Removing Ramification). *Suppose K has no ideal classes of order l^2 and does not contain ζ_l . If the Frattini embedding problem (G_K, ρ, α) has a solution ψ_0 , then it has a solution $\psi : G_K \rightarrow G$ with $\text{Ram}(\psi) \subset \text{Ram}(\rho) \cup T$.*

Proof:

The proof is similar to Lemma 6.2 of [3] except that we twist ψ_0 by a character of order l^e . Let $S = \text{Ram}(\psi_0) \setminus \{\text{Ram}(\rho) \cup T\}$, so if $v \in S$, then $\psi_0(I_v) \subseteq C$. Set $l^e = \max\{|\psi_0(I_v)| : v \in S\}$.

For $v \in S$ we define $\chi_v := \psi_0|_{I_v}$ viewed as $\chi_v : U_v \rightarrow \mu_{l^e}$ by reciprocity. By 6.1 there exists an idele class character χ of order l^e with certain local properties. We identify χ with $\eta : G_K \rightarrow C$ via reciprocity and set $\psi = \psi_0 \eta^{-1}$. Since the embedding problem (G_K, ρ, α) is Frattini, ψ is surjective. ■

Remark 6.4. Note that in case $e = 1$ the hypothesis on the order of ideal classes in the theorem above can be dropped.

7. FINDING AN m -SCHOLZ SOLUTION

We generalize Lemma 7.1 of [3] to prime powers.

Lemma 7.1. *Given integers $N \geq e \geq 1$, Galois l -extension L/K , characters $\chi_v : K_v^\times \rightarrow \mu_{l^e}$ for all v in a finite set $S \supseteq S_0$. Assume that K does not contain ζ_l . There exists a prime ideal \mathfrak{q} of K outside S and a character $\chi : J_K/K^\times \rightarrow \mu_{l^e}$ such that conditions (1)-(4) hold:*

- \mathfrak{q} splits completely in $L(\mu_{l^N})/K$
- $\chi|_{K_v^\times} = \chi_v$ for all $v \in S$.
- $\chi(U_{\mathfrak{q}}) = \mu_{l^e}$.
- $\chi(U_v) = 1$ for all $v \notin S \cup \{\mathfrak{q}\}$.

Proof:

Since S_0 is chosen large enough, we have $J_S/K_S \cong J/K^\times$. It therefore suffices to define a character $g : J_S \rightarrow \mu_{l^e}$ such that for all $(\alpha_v) \in J_S$

$$g((\alpha_v)) = \chi_{\mathfrak{q}}(\alpha_{\mathfrak{q}}) \times \prod_{v \in S} \chi_v(\alpha_v)$$

for some prime \mathfrak{q} and some epimorphism $\chi_{\mathfrak{q}} : U_{\mathfrak{q}} \rightarrow \mu_{l^e}$ chosen so that \mathfrak{q} splits completely in $L(\mu_{l^N})/K$ and $g(K_S) = \{1\}$.

We define a character $h : K_S \rightarrow \mu_{l^e}$ as the composition

$$K_S \xrightarrow{j} J_S \rightarrow \mu_{l^e}$$

where the left map j is the embedding of K_S in $\prod_{v \in S} K_v^\times$ and the right map is $\prod_{v \in S} \chi_v$. Thus for $x \in K_S$, $g(x) = h(x)\chi_{\mathfrak{q}}(x)$, so $\chi_{\mathfrak{q}}$ must be chosen to make $g(x) = 1$ for all $x \in K_S$.

Case $h(K_S) = \{1\}$. If \mathfrak{q} satisfies $K_S \subset U_{\mathfrak{q}}^{l^e}$, then for any character $\chi_{\mathfrak{q}} : U_{\mathfrak{q}} \rightarrow \mu_{l^e}$, we have $\chi_{\mathfrak{q}}(K_S) = \{1\}$. By Chebotarev's theorem, there exists a prime ideal $\mathfrak{q} \notin S$ of K which splits completely in $\Omega := L(\mu_{l^N}, \sqrt[l^e]{K_S})$. Note that \mathfrak{q} splitting completely in $K(\mu_{l^N})/K$ implies that absolute norm $N_{\mathbb{Q}}^K(\mathfrak{q}) \equiv 1 \pmod{l^N}$. Then $K_S \subseteq U_{\mathfrak{q}}^{l^e}$ by Kummer theory.

Case $h(K_S) \neq \{1\}$. The image $h(K_S)$ is cyclic of order l^k , $1 \leq k \leq e$. Thus there exists $x_1 \in K_S$ with $h(x_1)$ of order l^k . $K_S/K_S^{l^k}$ may be generated by $\{x_1, x_2, \dots, x_u\}$, with $h(x_i) = 1, i > 1$. By Burnside's basis theorem $\{x_1, \dots, x_u\}$ also generate $K_S/K_S^{l^e}$. We want to pick a prime $\mathfrak{q} \nmid l$, $\mathfrak{q} \notin S$ such that

- \mathfrak{q} splits completely in $L(\mu_{l^N})/K$.
- $x_1 \in U_{\mathfrak{q}}^{l^{e-k}} \setminus U_{\mathfrak{q}}^{l^{e-k+1}}$.
- $x_i \in U_{\mathfrak{q}}^{l^e}$ if $i > 1$.

To that end let

$$\Omega_k = L(\mu_{l^N}, \sqrt[l^{e-k}]{x_1}, \sqrt[l^e]{x_i} : i > 1).$$

The field Ω_k is a normal extension of K . By Lemma 4.2, $\text{Gal}(\Omega/L(\mu_{l^N})) \cong (\mathbb{Z}/l^e\mathbb{Z})^u$ and $\text{Gal}(\Omega/\Omega_k)$ is cyclic of order l^k . By Chebotarev's theorem we may choose $\mathfrak{q} \notin S$ such that $\text{Frob}(\mathfrak{q}, \Omega/K)$ generates $\text{Gal}(\Omega/\Omega_k)$, in particular \mathfrak{q} splits completely in Ω_k/K . This guarantees that the above three conditions on \mathfrak{q} are satisfied.

Having chosen \mathfrak{q} , we define $\chi_{\mathfrak{q}}$, a character of order l^e . Choose $y \in U_{\mathfrak{q}}$ such that $y^{l^{e-k}} = x_1 \in U_{\mathfrak{q}}$. We want $\chi_{\mathfrak{q}}(y)$ of order l^e , then $\chi_{\mathfrak{q}}(x_1)$ has order l^k . If $\beta = h(x_1)$ is an element of μ_{l^e} of order l^k , then $\beta = \alpha^{l^{e-k}}$, where α is a generator of μ_{l^e} . Set $\chi_{\mathfrak{q}}(y) = \alpha^{-1}$. Then $\chi_{\mathfrak{q}}(x_1) = \beta^{-1}$.

So we have chosen $\chi_{\mathfrak{q}}$ so that $\chi_{\mathfrak{q}}(x_1)h(x_1) = 1$. Thus $g(K_S) = 1$ and we have proved the lemma for prime power order characters. \blacksquare

Proposition 7.2. *Suppose that the central embedding problem (G_K, ρ, α) , G an l -group, is Frattini, ρ is l^N -Scholz, and $\zeta_l \notin K$. Assume there exists a solution ψ with $\text{Ram}(\psi) \cup T = \text{Ram}(\rho) \cup T$. Then there exists a prime $\mathfrak{q} \notin S := \text{Ram}(\psi) \cup S_0 \cup T$ and an l^N -Scholz solution φ such that $\text{Ram}(\varphi) = \text{Ram}(\psi) \cup \{\mathfrak{q}\}$.*

Proof:

Step 1. Define homomorphisms $\eta_v : D_v \rightarrow C$, $v \in S$.

- If $v \in S \setminus S_0$, we lift Frobenius at v to $\sigma_v \in D_v$. Since ρ is l^N -Scholz and $\text{Ram}(\psi) \cup T = \text{Ram}(\rho) \cup T$, after adjusting the lift σ_v we may assume $\psi(\sigma_v) \in C$ (see pg. 36 of [3]). Then let η_v be the unique homomorphism $D_v \rightarrow C$ satisfying $\eta_v(\sigma_v) = \psi(\sigma_v)$ and $\eta_v(I_v) = \{1\}$.

- If $v \in S_0$, $\alpha(\psi(D_v)) = \rho(D_v) = \{1\}$, again since ρ is l^N -Scholz. Thus $\psi(D_v) \subset \ker(\alpha) = C$. So define $\eta_v = \psi|_{D_v}$.

We have defined η_v , $v \in S$; now we apply Lemma 7.1 to get a map $\eta : G_K \rightarrow C$ and a prime $\mathfrak{q} \notin S$ such that $\eta|_{D_v} = \eta_v$, $v \in S$, $\eta(I_{\mathfrak{q}}) = C$, and η unramified for $v \notin \text{Ram}(\psi) \cup T \cup \{\mathfrak{q}\}$. Finally set $\varphi = \eta^{-1}\psi$. Note $\varphi(\sigma_v) = 1$, so $\varphi(D_v) = \varphi(I_v)$ if $v \in \text{Ram}(\psi) \cup T \setminus S_0$.

Step 2. We claim φ is unramified outside $\text{Ram}(\psi) \cup \{\mathfrak{q}\}$. In fact if $v \in S \setminus S_0$, we have $\eta(I_v) = \eta_v(I_v) = \{1\}$, so $\varphi(I_v) = \psi(I_v)$. The result follows.

Step 3. We claim φ is l^N -Scholz. Since the extension is Frattini, any solution is proper. The check of the three points of Definition 2.1 is similar to pg. 37 of [3] except for the proof that $\varphi(D_{\mathfrak{q}}) = \varphi(I_{\mathfrak{q}})$. For that, note that \mathfrak{q} is chosen to split completely in the fixed field of $\ker(\psi)$, so $\psi(D_{\mathfrak{q}}) = \{1\}$. Putting this together with $\eta(I_{\mathfrak{q}}) = C$, we conclude that $\varphi(D_{\mathfrak{q}}) = \varphi(I_{\mathfrak{q}})$. ■

Putting together Existence Theorem, Proposition 5.3, Proposition 6.3, Proposition 7.2 we have the next result.

Proposition 7.3. *Suppose $\zeta_l \notin K$ and K has no ideal classes of order l^2 . Given a central embedding problem (G_K, ρ, α) with G an l -group, cyclic C and ρ l^N -Scholz. If the extension is split or of Frattini type, then there exists an l^N -Scholz solution φ and a prime \mathfrak{q} of K such that*

$$\text{Ram}(\varphi) \cup T = \text{Ram}(\rho) \cup T \cup \{\mathfrak{q}\}.$$

Define the lower central series $\{G_i\}$ of G by $G_1 = G$, $G_{i+1} :=$ the commutator subgroup $[G_i, G]$, $i \geq 1$. If G is nilpotent, the smallest positive integer c such that $G_{c+1} = \{1\}$ is called the nilpotency class of G . Our main result below generalizes Proposition 2.5 of [10] who considers only the case $K = \mathbb{Q}$ and improves the result of Theorem 7.4 of [3] when the kernel C of the embedding problem is not of prime order.

Theorem 7.4. *Given a number field K , a prime l , and an l -group G of nilpotency class c . If G is nonabelian, suppose $\zeta_l \notin K$ and K has no ideal classes of order l^2 . Then*

$$\text{minram}_K(G) \leq d(G) + |T| + \sum_{i=2}^{c-1} d(G_i/G_{i+1}).$$

Remark 7.5. 1. This bound may be achieved by a tamely ramified extension L/K with $G \cong \text{Gal}(L/K)$. 2. If G is of nilpotency class 2,

$$\minram_K(G) \leq d(G) + |T|.$$

3. If we allow K to have ideal classes of order l^2 , then the bound has the form of [3]

$$\minram_K(G) \leq g + |T|, \quad |G| = l^g.$$

Proof:

As in Proposition 2.5 of [10] we use induction on i for a central embedding problem

$$1 \rightarrow G_i/G_{i+1} \rightarrow G/G_{i+1} \rightarrow G/G_i \rightarrow 1.$$

For $i = 1$, by Proposition 5.3 the embedding problem has an l^N -Scholz solution with at most $d(G^{ab}) = d(G)$ ramified primes. For $i \geq 1$, each extension is of Frattini type, and we may break the i -th problem up into $d(G_i/G_{i+1})$ cyclic Frattini problems. As shown in Proposition 7.3, each such problem may be solved at the cost of one more ramified prime. And since we can make the solution l^N -Scholz at each stage, it is guaranteed that we may solve the next embedding problem. ■

8. RAMIFICATION BOUND ON NILPOTENT GROUPS

We use the notation that a is the product of the primes dividing the order of G and integer N satisfies a^N is a multiple of the exponent of G . The purpose of this section is to extend Theorem 7.4 to groups $G = \prod_l G_l$ that are the direct product of their Sylow l -subgroups G_l , that is *nilpotent groups*. Assume $\zeta_l \notin K$ for all l dividing $|G|$. We will obtain G by a sequence of central embedding extensions with cyclic kernel; each of these extensions is a "product" of central extensions of l -groups as in sections 6 and 7. The nilpotent case was initially handled in the first author's thesis [8]. In this section we obtain an improved bound on $\minram_K(G)$ for fields K which do not contain ideal classes of order l^2 , where $l \mid |G|$.

The first step is to define a set T (as small as possible) of primes of K that contains an l^N -exceptional set T_l of primes for each l dividing $|G|$.

Let

$$\Omega_l = K(\sqrt[l^N]{E}, \sqrt[l]{V(l)})$$

as in 4.0.4 and let $\hat{\Omega} = \prod_{l|a} \Omega_l$. Since $\text{Gal}(\Omega_l(\mu_{a^N})/K(\mu_{a^N}))$ is an l -group, we have

$$(8.0.5) \quad \text{Gal}(\hat{\Omega}/K(\mu_{a^N})) \cong \prod_{l|a} \text{Gal}(\Omega_l(\mu_{a^N})/K(\mu_{a^N})).$$

Using the isomorphism of 8.0.5 we define

$$\sigma_i = \prod_{l|a} \sigma_i(l), \quad 1 \leq i \leq s \quad \text{and} \\ \tau_j = \prod_{l|a} \tau_j(l), \quad 1 \leq j \leq r$$

elements of $\text{Gal}(\hat{\Omega}/K(\mu_{a^N}))$. Here $r = \max_{l|a} r_l$ and we set $\tau_j(l) = 1$ if $r_l < j \leq r$. By Chebotarev's theorem, in K there is a set of $s+r$ prime ideals $T = \{\mathfrak{p}_i, \mathfrak{q}_j : 1 \leq i \leq s, 1 \leq j \leq r\}$ disjoint from any given finite set such that

$$\text{Frob}(\mathfrak{p}_i, \hat{\Omega}/K) = C(\text{Gal}(\hat{\Omega}/K), \sigma_i), \quad 1 \leq i \leq s \text{ and}$$

$$\text{Frob}(\mathfrak{q}_j, \hat{\Omega}/K) = C(\text{Gal}(\hat{\Omega}/K), \tau_j), \quad 1 \leq j \leq r.$$

Here $C(\text{Gal}(\hat{\Omega}/K), \gamma)$ denotes the conjugacy class of γ in $\text{Gal}(\hat{\Omega}/K)$. By the properties of the Frobenius, the restriction to Ω_l of σ_i (resp. τ_j) is $\sigma_i(l)$ (resp. $\tau_j(l)$) for each l dividing a .

Lemma 8.1. *We continue the notation of Corollary 4.3 and Lemma 4.2. For each $l|a$, let L_l be an l^N -Scholz l -extension of K fixed by the kernel of homomorphism $\rho_l : G_K \rightarrow \tilde{G}_l$ and let (G_K, ρ_l, α_l) be a Frattini central embedding problem as in (2.0.1). Assume for all $l|a$, that ζ_l is not in K and the exponent of G_l divides l^N . When $|\ker(\alpha_l)| > l$, assume additionally that no ideal class of K has order l^2 . Then for each $l|a$ there exists a solution*

$$\phi_l : G_K \rightarrow G_l$$

for which $\text{Ram}(\phi_l) \subseteq \text{Ram}(\rho_l) \cup T$.

Proof:

The existence of any solution is Lemma 3.1. Our set of primes T contains l^N -exceptional subsets T_l , hence we may apply Theorem 6.3 to get a solution ϕ_l such that $\text{Ram}(\phi_l) \subseteq \text{Ram}(\rho_l) \cup T$ for all primes $l|a$. ■

In the next lemma we apply Corollary 4.4 to find a single prime \mathfrak{q} that we use to lift local characters indexed by $l|a$.

Lemma 8.2. *Let S be a finite set of primes of K that contains S_0 . For each prime $l|a$, we are given integers e_l , $N \geq e_l \geq 1$, Galois l -extension L_l/K , character $\chi_{v,l} : K_v^\times \rightarrow \mu_{l^{e_l}}$ for all $v \in S$. Assume that K does not contain ζ_l for each $l|a$. There exists a prime ideal \mathfrak{q} of K outside S and idele class characters*

$\chi_l : J_K/K^\times \rightarrow \mu_{l^{e_l}}$ such that conditions (1)-(4) hold for all $l|a$:

- \mathfrak{q} splits completely in $L_l(\mu_{l^N})/K$
- $\chi_l|_{K_v^\times} = \chi_{v,l}$ for all $v \in S$.
- $\chi_l(U_{\mathfrak{q}}) = \mu_{l^{e_l}}$.
- $\chi_l(U_v) = 1$ for all $v \notin S \cup \{\mathfrak{q}\}$.

Proof:

Let R_l denote the field $L_l(\sqrt[l^N]{K_S})$, $R = \prod_{l|a} R_l$, $\Gamma_l = \text{Gal}(R_l/K)$ and $\Gamma = \text{Gal}(R/K)$.

In Lemma 7.1, for all $l|a$ we have defined a special prime \mathfrak{q}_l (not to be confused with \mathfrak{q}_i 's defined in Definition 4.5). Define $\sigma_l \in \Gamma_l$ by $\text{Frob}(\mathfrak{q}_l, R_l/K) = C(\Gamma_l, \sigma_l)$. Next we show that a single prime \mathfrak{q} can be chosen. By Lemma 4.4 there exists an element $\sigma \in \Gamma$ whose restriction to R_l equals σ_l for all $l|a$. By Chebotarev's theorem, there exists a prime \mathfrak{q} of K outside S such that $\text{Frob}(\mathfrak{q}, R/K) = C(\Gamma, \sigma)$. By restriction $\text{Frob}(\mathfrak{q}, R_l/K) = C(\Gamma_l, \sigma_l)$ for all $l|a$ and conditions (1)-(4) of 8.2 are satisfied. ■

Remark 8.3. The method by which we replaced $\{\mathfrak{q}_l : l|a\}$ by \mathfrak{q} is similar to that where we replaced $\{T_l : l|a\}$ by T .

Theorem 8.4. *Given a number field K and a finite nilpotent group G of class c . If G is nonabelian, suppose $\gcd(|G|, |\mu_K|) = 1$ and assume for all primes dividing $|G|$ that the ideal class group of K has no elements of order l^2 . Then*

$$\minram_K(G) \leq d(G) + (r + s) + \sum_{i=2}^{c-1} d(G_i/G_{i+1}).$$

Here $s = \mathbb{Z}$ -rank of units of K and $r = \max_{l||G|} \{\dim Cl(K)_l\}$.

Proof:

By Corollary 5.2 it remains to prove the result for nonabelian groups G . Since G is nilpotent, for each l dividing $|G|$, we may apply Propositions 7.2, 7.3, Theorem 7.4 inductively. By Lemma 8.2 there exists a single prime \mathfrak{q} to which Proposition 7.2 may be applied, and the conclusion follows. \blacksquare

9. SCHUR EXTENSIONS

In this section we use Fröhlich's result on realizing the Schur multiplier without additional ramification to verify Boston's conjecture [1] for a certain class of l -groups given by central extensions

$$1 \rightarrow \mathcal{M}(\Gamma) \rightarrow G \rightarrow \Gamma \rightarrow 1.$$

In addition Theorem 9.7 confirms Boston's conjecture for a particular G of exponent l , and includes the determination of the central class field of any finite abelian extension L/\mathbb{Q} of exponent l that is its own genus field.

The group $\mathcal{M}(\Gamma)$ is the Schur multiplier of a profinite group Γ as defined in [2].

Definition 9.1. Suppose $M \supseteq L \supseteq K$ are number fields with M/K and L/K Galois extensions. Let M' be the maximal central extension of L/K in M and let E be the maximal abelian extension of K in M . Fröhlich defines a certain surjective homomorphism

$$(9.0.6) \quad \mathcal{M}(\text{Gal}(L/K)) \rightarrow \text{Gal}(M'/EL).$$

If it is an isomorphism, one says that M realizes the multiplier $\mathcal{M}(\text{Gal}(L/K))$.

Remark 9.2. If central extensions M_1 and M_2 for L/K both realize the multiplier of $\text{Gal}(L/K)$, the Galois groups $\text{Gal}(M_i/K)$, $i = 1, 2$ need not be isomorphic.

Fröhlich in Proposition 3.2 of [2] proves that if L/K is an extension of finite degree, there is a finite degree central extension M of L/K that realizes $\mathcal{M}(\text{Gal}(L/K))$.

For a prime l and a finite set of primes S of K , $K(l, S)$ denotes the maximal l -extension field of K with ramification restricted to S , and $K(l, S)^{ab}$ is the maximal abelian subextension of $K(l, S)$. If S contains no divisors of l , then the degree $[K(l, S)^{ab} : K]$ is finite. From now on suppose L/K is a finite degree l -extension, so $\mathcal{M}(\text{Gal}(L/K))$ is a finite abelian l -group. Let S be the set of primes of K ramified in L . For $K = \mathbb{Q}$ (resp. K imaginary quadratic with $\zeta_l \notin K$), Fröhlich in Corollary 2 of Theorem 3.13 in [2], (resp. Watt in Theorem 3.1 of [14]) proved in addition

there exists such an extension M that is ramified at worst at primes above S (the key result on which Theorem 9.4 is based). Since M is central for L/K , we have $M = M'$. Furthermore if $L \supseteq K(l, S)^{ab}$, then $L \supseteq E$, so $EL = L$ and 9.0.6 asserts

$$\mathcal{M}(\text{Gal}(L/K)) \cong \text{Gal}(M/L).$$

Remark 9.3. Fröhlich does not require L/K to be an l -extension.

Thus from the results of Fröhlich and Watt we have the following theorem.

Theorem 9.4. *Let K be \mathbb{Q} or imaginary quadratic with $\zeta_l \notin K$ and let L/K be a finite Galois l -extension tamely ramified only at S ; suppose $L \supseteq K(l, S)^{ab}$. Then there exists a central extension M of L/K with $\text{Ram}(M/K) \subseteq S$ such that $\mathcal{M}(\text{Gal}(L/K)) \cong \text{Gal}(M/L)$.*

■

Remark 9.5. We may apply the theorem repeatedly by replacing the extension L/K by M/K .

Remark 9.6. Since the number of generators of $\text{Gal}(K(l, S)/K)$ equals the number of generators of $\text{Gal}(K(l, S)^{ab}/K)$, we have that $\text{Gal}(L/K)$ and $\text{Gal}(M/K)$ have the same number of generators.

Theorem 9.7. *Let l be an odd prime and let G be a group generated by x_1, \dots, x_n subject to relations $x_i^l = 1$, $[x_i, x_j] \in Z(G) = \text{center of } G$ for all i, j . There exists a tamely ramified extension M/\mathbb{Q} such that $\text{Gal}(M/\mathbb{Q}) \cong G$ and $|\text{Ram}(M/\mathbb{Q})| = n$. Moreover M is the central class field of its maximal abelian subfield M^{ab} .*

Proof:

Note that $\mathcal{M}(G/Z(G)) \cong Z(G)$.

By Proposition 2.5 of [10] there exists an extension M/\mathbb{Q} such that $\text{Gal}(M/\mathbb{Q}) \cong G$ which is (tamely) ramified at n primes. Moreover we have $\text{Ram}(M/\mathbb{Q}) = \text{Ram}(M^{ab}/\mathbb{Q})$.

Next we show that M/M^{ab} is actually unramified. Suppose a prime ramifies in M/M^{ab} . As it also ramifies in M^{ab}/\mathbb{Q} , it follows that its ramification index is divisible by l^2 . Note that since M/\mathbb{Q} is tamely ramified, all ramification groups are cyclic. But that gives a contradiction to the exponent l of G , thus M is unramified over M^{ab} .

Clearly $\text{Gal}(M^{ab}/\mathbb{Q})$ is the direct product of its inertia subgroups; by a standard result M^{ab} is its own genus field. As $\text{Gal}(M/M^{ab})$ lies in the center of $\text{Gal}(M/\mathbb{Q})$, M is contained in the central class field Z of M^{ab} . From e.g. [5], the degree of Z over M^{ab} divides $l^{n(n-1)/2} = [M : M^{ab}]$. Hence $M = Z$.

■

Remark 9.8. In the theorem above M realizes the multiplier $\mathcal{M}(\text{Gal}(M^{ab}/\mathbb{Q}))$.

Remark 9.9. Fröhlich [2] Theorem 5.1 has determined the Galois group of the central class field of any abelian l -extension of \mathbb{Q} by a different method.

The second author thanks Marcin Mazur for a useful discussion regarding Lemma 4.1.

REFERENCES

- [1] Nigel Boston and Nadya Markin. The fewest primes ramified in a G -extension of \mathbb{Q} , 2010.
- [2] Albrecht Fröhlich. *Central extensions, Galois groups, and ideal class groups of number fields*, volume 24 of *Contemporary Mathematics*. American Mathematical Society, Providence, RI, 1983.
- [3] Wulf-Dieter Geyer and Moshe Jarden. Bounded realization of l -groups over global fields. The method of Scholz and Reichardt. *Nagoya Math. J.*, 150:13–62, 1998.
- [4] Georges Gras. *Class field theory*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2003. From theory to practice, Translated from the French manuscript by Henri Cohen.
- [5] Mitsuko Horie. On central extensions of elementary abelian fields. *J. Number Theory*, 36(1):95–107, 1990.
- [6] Hershy Kisilevsky and Jack Sonn. On the minimal ramification problem for ℓ -groups, 2008.
- [7] H. Koch. *Galoissche Theorie der p -Erweiterungen*. Springer-Verlag, Berlin, 1970. Mit einem Geleitwort von I. R. Šafarevič.
- [8] Nadya Markin. Galois groups with restricted ramification, 2006.
- [9] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008.
- [10] Bernat Plans. On the minimal number of ramified primes in some solvable extensions of \mathbb{Q} . *Pacific J. Math.*, 215(2):381–391, 2004.
- [11] Karl Rubin. The one-variable main conjecture for elliptic curves with complex multiplication. In *L -functions and arithmetic (Durham, 1989)*, volume 153 of *London Math. Soc. Lecture Note Ser.*, pages 353–371. Cambridge Univ. Press, Cambridge, 1991.
- [12] Jean-Pierre Serre. *Topics in Galois theory*, volume 1 of *Research Notes in Mathematics*. A K Peters Ltd., Wellesley, MA, second edition, 2008. With notes by Henri Darmon.
- [13] I.R. Shafarevich. *Extensions with Given Points of Ramification*, volume 18 of *Inst. Hautes Etudes Sci. Publ. Math.* 1963.
- [14] Stephen B. Watt. Restricted ramification for imaginary quadratic number fields and a multiplier free group. *Trans. Amer. Math. Soc.*, 288(2):851–859, 1985.

E-mail address: `nadyaomarkin@gmail.com`

E-mail address: `ullom@math.uiuc.edu`

NADYA MARKIN, CASL UCD, BELFIELD, DUBLIN, IRELAND

STEPHEN ULLOM, 1409 WEST GREEN ST UNIVERSITY OF ILLINOIS URBANA, IL 61801, USA